REMARKS/ARGUMENTS

In response to the Examiner's objection to the Abstract as being too long, Applicant has provided an amended Abstract which meet the requirements of 37 CFR 1.72(b).

In response to the Examiner's objection to Figures 1, 2 and 3 Applicant has attached herewith replacement drawings in which the lines are uniform and solid.

The Examiner has rejected claims 1 - 9, 11, 13-21 and 23 under 35 USC 102(e) as being anticipated by **Hayden** (US 6,018,771). Applicant respectfully disagrees for the reasons that follow.

As specified in the title, Applicant's invention applies to protecting the Internet which is an IP based WAN with hundreds of millions of computer hosts all interconnected through IP protocols at the network and transport layers. The system relies on existing IP protocols including routing protocols through conventional border routers. The key feature of Applicant's invention is that it relies on the use of rapidly changing IP based multicast addresses in a hopping sequence known **only** to the receiving and transmitting stations which are topologically distributed within the Internet. The hopping sequence of rapidly changing multicast addresses and the time slots at which these addresses are used are only known only to the transmitting and receiving stations. The sequence is selected or generated, usually through a defined cryptographic process, such that to an outside attacker, there is no obvious predictable sequence of addresses and time slots. Since the IP multicast protocol is based on a subscriber or "pull" protocol rather than the "push" protocol used for unicast, it is very difficult for an attacker to flood a site since he must know the sequence and timing for the multicast addresses. This system is analogous to frequency hopping spread spectrum anti jamming radio systems.

Applicant has amended the claims to emphasize that the multicast address hopping technique provides rapidly changing multicast addresses to specified subscriber such that any

potential attacker is unable to successfully disrupt or monitor for traffic between end stations. In claim 1 for example, Applicant has indicated that a multicast address hopping method is being claimed in which the multicast address hopping scheme is known only to transmitter and subscriber end stations within the multicast group. Further, the multicast address hopping scheme is initiated by a cryptographic key.

The Examiner has relied heavily in the **Hayden** reference to support both the novelty and obvious objections raised. It must be emphasized from the outset that **Hayden** is not even remotely concerned with preventing denial of service attacks or Internet security generally, both of which are the focus of Applicant's invention. Further, Hayden does not provide a multicast address hopping technique in which unsubscribed users are not privy to the address hopping scheme. **Hayden** specifically relates to the dynamic assignment, deassignment, and reassignment of a common pool of allocated multicast addresses to multiple users for varying data streams (see col. 7 lines 65 and 66). This patent is concerned with the ability to share a limited pool of available multicast addresses among multiple users in a **publicly** advertised fashion (see col 2 lines 44 to 60). Furthermore, this patent applies to link or physical layer multicast addressing on a Local Area Network LAN), not multicast on an Internet Protocol (IP) based Wide Area Network (WAN)). Applicant's notes that there are normally a limited number of multicast addresses available at the physical and link level which are used in a LAN (depending on any subnet masking scheme). This is not the case for IP based networks where there are over 130 million potential multicast addresses available. **Hayden** is only applicable to LAN and would not work in the IP WAN topology associated with the present invention. As highlighted at col 1, line 58 and col 3, lines 18 to 34, **Hayden** specifically references a LAN and LAN protocols respectively. This is further evidenced by the description of the network structure at col 3, lines 20 to 23.. **Hayden** does not refer to IP multicast protocols, including WAN protocols, despite the fact that such protocols were known at the time of the application as evidenced by the publicly available "Request for Comment (RFC) 1112 Host Extensions for IP multicasting, S. Deering, Stanford University, dated August 1989". Applicant also notes that the **Hayden** application was originally made in 1992 before IP networking was widely used. In short, adopting the LAN system of **Hayden** to an IP WAN environment is a non-trivial task requiring inventive ingenuity beyond simple workshop engineering. More specifically, the

Hayden system would not scale to a WAN because, for example, it would not be possible to have the process described at col 4, lines 26 to 65 work on an IP based WAN since it would be impossible to have every client on the Internet able to monitor all announcement packets of every multicast server on the Internet due to the sheer volume of traffic and processing power required. This is why the IP Multicast protocols described in RFC 1112 mentioned above were developed and are implemented within IP WANs.

With respect to the portions of the description cited by the Examiner, Applicant respectfully submits that the Examiner has misunderstood the invention disclosed in Hayden. Col 1 lines 65-67 and col 2 lines 1-20 refers to dynamic address allocation not a predetermined scheme known only to end stations. Further, col 2 lines 8-35 highlights that the dynamic address allocation system of **Hayden** relies on a public announcement scheme to advertise not hide address in use. Still further, col 2. lines 44-57 referred to by the Examiner deals with the reuse of multicast addresses by varying addresses that are not in use, not the deliberate varying the address to prevent attacks.

In light of the above, Applicant respectfully requests reconsideration and removal of the 25 USC 102(e) rejection.

The Examiner has rejected claims 10 and 22 under 35 USC 103(a) as being unpatentable over **Hayden** in view of **Caronni** (US 6,049,878). Applicant respectfully disagrees for the reasons that follow.

Caronni deals specifically with a method for the management and distribution of group keys to encrypt individual datagrams or packets used in a multicast network, for example the IP based Internet. Group keys are needed when there are multiple recipients for transmission of encrypted data from a source. **Caronni** is concerned with the confidentiality aspects of protection of data through encryption not with the protection of the availability of data against Denial of Service attacks as described in the present application. Specifically, **Caronni** at col 7 lines 40 -52 describes the preferred use of a dedicated unicast link (that is a physical link

separate from the actual network using the secure multicast system described by **Caronni**). This link would be used to securely send new keys so that the keys are not subject to eavesdropping nor other type of attacks (e.g. Man in the Middle) during transit on a publicly accessible network, e.g. the Internet. **Caronni** describes a method to eliminate keys to prevent replay attacks at col 9 lines 57-65 but the reference to attacks here does not deal with denial of service attacks as described in the present application but refers rather to replay attacks whereby an encrypted packet is captured by an attacker, stored for a period of time, then replayed in hopes that the key is still valid and the packet will be decrypted and delivered to the destination a second time which can cause various detrimental effects. **Caronni** does not describe a method of identifying and filtering unicast datagrams implementing a denial of service attack, (e.g. a packet storm clogging the physical communication link) on a site through the network. It describes the use of a separate physical link (e.g. dial up telephone link) to protect the keys from active attack. The present application does not claim the key distribution nor packet encryption technology.

When the comments relating to **Hayden** are considered in light of the comments relating to **Caronni**, Applicant submits that the combination of **Hayden** and **Caronni** do not make Applicant's invention as claimed in claims 10 and 22 obvious. Reconsideration and removal of the 35 USC 103(a) objection is respectfully requested.

The Examiner has rejected claims 12 and 24 under 35 USC 103(a) as being unpatentable over **Hayden** in view of **Li** (US 6,606,706). Applicant respectfully disagrees for the reasons that follow.

Li is concerned with cryptographically separating multicast traffic in a hierarchical system to create separate security domains. It does describe the use of border routers, however Applicant notes that these are not conventional border routers running standard IP multicast routing protocols as used in the present application, but are more correctly referred to as "security domain border routers" which in effect are not conventional "border routers" but contain specialized functionality, likely implemented in a special device. These devices, as described in **Li** col 2 lines 28-48, implement a tunneling protocol to allow encrypted multicast packets to

traverse a lower level security domain. This specialization is highlighted in **Li** at col 12 lines 42-67 and col 13 lines 1-12. These "security domain border routers" are not concerned with efficient routes but rather the correct security of the multicast security domains and would use the underlying conventional multicast protocols on the conventional "border routers" to perform efficient routing.

When the comments relating to **Hayden** are considered in light of the comments relating to **Li**, Applicant submits that the combination of **Hayden** and **Li** do not make Applicant's invention as claimed in claims 12 and 24 obvious. Reconsideration and removal of the 35 USC 103(a) objection is respectfully requested.

It is also worth noting that the inventions of **Caronni** and **Li** are applicable to the Internet while, as already discussed, **Hayden** is applicable to a Local Area Network. Applicant submits that there is not motivation to combine these two references, since one skilled in the art would not look to combine LAN technology with Internet technology to achieve Applicant's invention.

Based on the above-noted arguments and amendments, Applicant submits that the application is now in good order and ready for allowance.

Respectfully submitted,
Shawcross, Charles

By _____
Allan Millard
Reg. 43,397
Tel. 1-613-238-6404

Cassan Maclean
80 Aberdeen Street
Ottawa, Ontario
K1S 5R5
February 6, 2004

APPENDIX

This Page Blank (uspto)